

AMENDED IN ASSEMBLY MAY 13, 2003

AMENDED IN ASSEMBLY APRIL 30, 2003

AMENDED IN ASSEMBLY APRIL 21, 2003

CALIFORNIA LEGISLATURE—2003–04 REGULAR SESSION

ASSEMBLY BILL

No. 1387

Introduced by Assembly Member Yee

February 21, 2003

An act to add Sections 9174, 9926, 9927, 9928, and 9929 to the Government Code, relating to the Legislature.

LEGISLATIVE COUNSEL'S DIGEST

AB 1387, as amended, Yee. Legislature.

Under existing law, each house of the Legislature appoints its own employees.

This bill would require that each house of the Legislature use a unique number other than an individual's social security number to identify its employees, beginning January 1, 2005.

Under existing law, state agencies in the executive branch are required to establish a permanent privacy policy that includes certain provisions.

This bill would require that each house of the Legislature establish and maintain a permanent privacy policy that includes the principles set forth in existing law for state agencies. The bill would also require each house to provide specified notice to persons before collecting personal information, to establish rules for persons using this personal information, to establish safeguards to protect the confidentiality of the

personal information, and to provide notification of any breach in security.

The provisions of this bill would become operative on January 1, 2005.

Vote: majority. Appropriation: no. Fiscal committee: no. State-mandated local program: no.

The people of the State of California do enact as follows:

1 SECTION 1. Section 9174 is added to the Government Code,
2 to read:

3 9174. On and after January 1, 2005, each house of the
4 Legislature shall use a unique identifying number other than an
5 individual's social security number to identify its employees.

6 SEC. 2. Section 9926 is added to the Government Code, to
7 read:

8 9926. (a) Each house of the Legislature shall establish and
9 maintain a permanent privacy policy that includes, but is not
10 limited to, the following principles:

11 (1) Personally identifiable information is obtained only
12 through lawful means.

13 (2) The purposes for which personally identifiable data are
14 requested are specified at or prior to the time of collection, and any
15 subsequent use is limited to the fulfillment of purposes not
16 inconsistent with those purposes previously specified.

17 (3) Personal data is not disclosed, made available, or otherwise
18 used for purposes other than those specified, except with the
19 consent of the subject of the data, or as authorized by statute,
20 regulation, rule, or policy adopted by the Committee on Rules of
21 the house.

22 (4) Personal data collected is relevant to the purpose for which
23 it is collected.

24 (5) The general means by which personal data is protected
25 against loss, unauthorized access, use modification, or disclosure
26 is posted, unless that disclosure of general means would
27 compromise legitimate objectives of either house of the
28 Legislature or law enforcement purposes.

29 (b) Each house of the Legislature shall designate a position
30 within the house, the duties of which shall include, but not be
31 limited to, responsibility for the privacy policy within that house.



1 SEC. 3. Section 9927 is added to the Government Code, to
2 read:

3 9927. Each house of the Legislature shall provide, on or with
4 any form used to collect personal information from individuals,
5 the notice specified in this section. When contact with the
6 individual is of a regularly recurring nature, an initial notice
7 followed by a periodic notice at least once per session satisfies this
8 requirement. This requirement is also satisfied by notification
9 each session to individuals of the availability of the notice. The
10 notice shall include all of the following:

11 (a) The title, business address, and telephone number of the
12 official who is responsible for the system of records.

13 (b) The authority, whether granted *or required* by statute,
14 regulation, rule, or policy adopted by the Committee on Rules of
15 the house, that authorizes *or requires* the maintenance of the
16 information.

17 (c) With respect to each item of information, whether
18 submission of the information is mandatory or voluntary.

19 (d) The consequences, if any, of not providing all or any part
20 of the requested information.

21 (e) The principal purpose or purposes within the Legislature
22 for which the information is to be used.

23 The notice required by this section does not apply to
24 requirements for an individual to provide his or her name,
25 identifying number, photograph, address, or similar identifying
26 information if this information is used only for the purpose of
27 identification and communication with the individual by the
28 Legislature, except that requirements for an individual's social
29 security number shall conform to the provisions of state and
30 federal law. The notice required by this section does not apply to
31 the Legislature when it uses forms adopted by another state
32 agency.

33 SEC. 4. Section 9928 is added to the Government Code, to
34 read:

35 9928. (a) Each house of the Legislature shall establish rules
36 of conduct for persons involved in the design, development,
37 operation, disclosure, or maintenance of records containing
38 personal information, and instruct each such person with respect
39 to those rules.

(b) Each house of the Legislature with the assistance of the Legislative Counsel shall establish appropriate and reasonable administrative, technical, and physical safeguards to ensure the security and confidentiality of records consistent with existing law, and to protect against anticipated threats or hazards to their security or integrity that could result in any injury.

SEC. 5. Section 9929 is added to the Government Code, to read:

9929. (a) If a house of the Legislature owns or has license to computerized data that includes personal information, following discovery or notice of any breach in the security of its computerized data system the house shall notify any person whose unencrypted personal information was, or is reasonably believed to have been, thereby acquired by an unauthorized person. The notification shall be made in the most expedient time possible and without unreasonable delay, consistent with subdivision (c) and any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system. Following discovery or notice of a breach in the security of the Legislature's computerized data systems, the Legislative Counsel shall notify the affected house of the Legislature in the most expedient time possible and without unnecessary delay. Unless the Legislature discovers or is notified of a breach by other means, the Legislature shall not be required to make the notification to persons whose unencrypted personal information was, or is believed to have been, acquired by an unauthorized person, until the Legislature receives notice of the breach from the Legislative Counsel.

(b) If a house of the Legislature maintains computerized data that includes personal information that the house does not own or have license to, immediately following discovery or notice of any breach in the security of its computerized data system the house shall notify the owner or licensee of any personal information that was, or is reasonably believed to have been, thereby acquired by an unauthorized person.

(c) The notification required by this section may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation.

(d) For purposes of this section, "breach in the security" of a system means the unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of

1 personal information maintained by the house of the Legislature.
2 Good faith acquisition of personal information by an employee or
3 agent of either house of the Legislature for the purposes of the
4 house is not a breach of the security of the system, provided that
5 the personal information is not made subject to unauthorized
6 disclosure.

7 (e) For purposes of this section, “personal information” means
8 a person’s first name or first initial and last name in combination
9 with one or more of the following data elements, when either the
10 name or the data element or elements are not encrypted:

11 (1) The person’s social security number.

12 (2) The person’s driver’s license number or California
13 identification card number.

14 (3) The person’s account number, credit or debit card number,
15 in combination with any required security code, access code, or
16 password that would permit access to the person’s financial
17 account.

18 (f) For purposes of this section, “personal information” does
19 not include information that is lawfully made available to the
20 general public from federal, state, or local government records.

21 (g) For purposes of this section, notification may be provided
22 by one of the following methods:

23 (1) Written notice.

24 (2) E-mail.

25 (3) Electronic notice, if the notice provided is consistent with
26 the provisions regarding electronic records and signatures set forth
27 in Section 7001 of Title 15 of the United States Code.

28 (4) Substitute notice, if the cost of providing notice would
29 exceed two hundred fifty thousand dollars (\$250,000), or the
30 affected class of subject persons to be notified exceeds 500,000,
31 or the house of the Legislature does not have sufficient contact
32 information. Substitute notice may be provided by performing
33 both of the following:

34 (A) Conspicuous posting of the notice on the Web site page of
35 each house of the Legislature.

36 (B) Notification to major statewide media.

37 (h) Notwithstanding subdivision (g), if a house of the
38 Legislature maintains its own notification procedures as part of an
39 information security policy for the treatment of personal
40 information and its procedures are consistent with the timing

1 requirements of this section, it shall be deemed to be in compliance
2 with the notification requirements of this section if it notifies
3 subject persons in accordance with its policies in the event of a
4 breach in the security of the system.

5 SEC. 6. The provisions of this act shall become operative on
6 January 1, 2005.

O

